

FEDERAL BUREAU OF INVESTIGATION**Precedence:** ROUTINE**Date:** 08/24/1998**To:** Cincinnati**Attn:** [redacted]**From:** NSD

NIPC/CIOS/CIU/11719

Contact: SSA [redacted]

b6
b7C**Approved By:** [redacted]**Drafted By:** [redacted]**Case ID #:** 288-CI-68562 (Pending)**Title:** UNSUB(S);UNITED STATES AIR FORCE
INSTITUTE OF TECHNOLOGY - VICTIM;
CITA - COMPUTER INTRUSION;
OO: CINCINNATI**Synopsis:** This communication is to forward documents to the original case file.

Referral/Consult

Enclosure(s): Two copies of Request For Information letters sent to [redacted] One copy of response from NAVCIRT regarding possible material related to captioned matter.**Details:** Enclosed for Cincinnati are copies of documents generated by or directed to the National Infrastructure Protection Center (NIPC) regarding captioned matter. These documents are being forwarded to Cincinnati for inclusion in the original case file.

♦♦

288-CI-68562-21

SEARCHED	INDEXED
SERIALIZED	FILED
[Redacted]	
[Signature]	

b6
b7C

U.S. Department of Justice



Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 4, 1998



Dear [redacted]

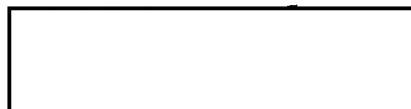
Referral/Consult

This letter is to request information from [redacted] databases and published reports that may be relevant to an ongoing FBI criminal investigation. The investigation centers on a series of intrusions into computer systems located at Wright Patterson Air Force Base. The intrusions appear to originate from a series of Internet service providers located in the Russian Federation. It also appears that the intruder is connecting to the ISPs through a "dial-up" connection, which suggests a local (i.e. Russian) point of origin. The FBI currently possesses no information indicating that the attacker is a U.S. person.

Technical information relevant to this request is provided in the enclosure, which also specifies an operational point of contact in the FBI. As additional technical information becomes available, it will be forwarded to the operational point of contact at [redacted]

The FBI legal contact point for this matter is Assistant General Counsel [redacted]
[redacted] Please do not hesitate to call him if you require additional information.
Thank you for your assistance in this matter.

Sincerely,



b6
b7C

Associate General Counsel for National
Security Affairs

cc: [redacted]

[redacted] OGC/NIPC

The Wright Patterson Air Force Base (WPAFB), a key educational and research and development base, has documented numerous intrusions into approximately eight of their systems. The attacks primarily come through computers located in the computer lab at the University of Cincinnati. However, attacks have been seen from Wright University, located in Dayton, OH and Aticorp.net located in Charleston, SC. The intrusions into these U.S. systems appears to be originating from a dialup connection to four Internet Service Providers (ISPs) located in Russia. The hacking occurs Monday through Friday, midnight and approximately 9:00 a.m. EDT.

The following are the [redacted] involved:



b7E

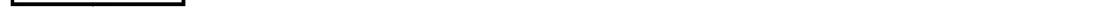
The following passwords or environment variables have been used during the intrusions:



b6
b7C

The following are usernames, software authors or tool names:

[redacted] [redacted] is the name of [redacted] student whose account is being used at [redacted] Our information indicates she is a non-U.S. person.)
[redacted]



The following files are known to have been taken by the hacker from WPAFB:



b7E

NIPC Operational POC is SSA [redacted]

b6
b7C

U.S. Department of Justice



Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 3, 1998



Referral/Consult

Dear [redacted]

This letter is to request information from [redacted] databases and published reports that may be relevant to an ongoing FBI criminal investigation. The investigation centers on a series of intrusions into computer systems located at Wright Patterson Air Force Base. The intrusions appear to originate from a series of Internet service providers located in the Russian Federation. It also appears that the intruder is connecting to the ISPs through a "dial-up" connection, which suggests a local (i.e. Russian) point of origin. The FBI currently possesses no information indicating that the attacker is a U.S. person.

Technical information relevant to this request is provided in the enclosure, which also specifies an operational point of contact in the FBI. As additional technical information becomes available, it will be forwarded to the operational point of contact at [redacted]

The FBI legal contact point for this matter is Assistant General Counsel [redacted]
[redacted]. Please do not hesitate to call him if you require additional information.
Thank you for your assistance in this matter.

Sincerely,

[redacted]
Associate General Counsel for National
Security Affairs

cc: [redacted] OGC/NIPC
NSA

b6
b7C

~~SECRET~~



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 31, 1998



Dear [redacted]

Referral/Consult

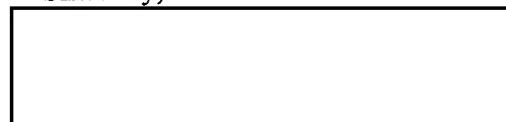
This letter is to request [redacted] technical assistance in conjunction with an ongoing FBI criminal investigation. The investigation centers on a series of intrusions into computer systems located at Wright Patterson Air Force Base. The intrusions appear to originate from a (U) series of Internet service providers located in the Russian Federation. It also appears that the intruder is connecting to the ISPs through a "dial-up" connection, which suggests a local (i.e. Russian) point of origin. The FBI currently possesses no information indicating that the attacker is a U.S. person. (S)

The FBI has already made (in an August 21, 1998, letter addressed to Acting General Counsel [redacted] a standard Request for Information in connection with this (U) investigation. The purpose of this letter is to add a technical assistance request so that [redacted] expert personnel can assist the FBI investigators on certain technical questions relating to computer data collected by the FBI. (S)

b6
b7C

The FBI legal contact point for this matter is Assistant General Counsel [redacted]
[redacted] Please do not hesitate to call him if you require additional information.
Thank you for your assistance in this matter. (U)

Sincerely,



b6
b7C

Associate General Counsel for National Security Affairs

cc: [redacted]

Referral/Consult

Derived From: Multiple Sources
Declassify on: X1

688-CI-68562-22

SEARCHED	INDEXED
SERIALIZED	FILED
FBI - CINCINNATI	

[Handwritten signatures and initials over the stamp]

~~SECRET~~